Department of Indian Affairs and Northern Development
Departmental Audit and Evaluation Branch

Prepared by:

Hasan Zaidi, Audit Manager
Hélène Thériault, Project Manager

Departmental Audit and Evaluation Branch

Assisted by:
Performance Management Network

Audit of Security

Project 96/06
June 1997

Table of Contents

Page

Executive Summary ..... **i**
- Purpose i
- Background i
- Overall Assessment i
- Key observations i

Section 1 - Introduction **1**
- Background 1
- Objectives 1
- Scope 1

Section 2 - Observations and Recommendations **2**
- Security Environment 2
- Management Framework 4
- Security Program 6

Appendix 1 8

Appendices
- Terms of reference
- Action plan

Purpose

The purpose of this audit is to provide a comprehensive assessment of the management and administration of the departmental security function; and compliance with the Government Security Policy (GSP) and the Information Technology Security (IT) operational standards.

Background

The department must conduct internal audits of compliance with, and effectiveness and efficiency of the implementation of the Government Security Policy (GSP) every five years. The previous audit in 1992-1993 identified that a number of improvements were required to strengthen management and delivery practices and to comply to the requirement of the GSP.

Overall Assessment

The departmental security function has improved in comparison to conditions observed during the 1992 audit. The implementation of Threat and Risk Assessments, security awareness programs and other initiatives have strengthened the function. However, in most locations visited, the concern for security is still low, resulting in assets, particularly sensitive information, not being safeguarded adequately.

The need to further strengthening the security function to be within an acceptable level of risk will require changes to security procedures, but mostly in people's attitudes.

Key observations

The department needs to upgrade the efficiency of its annual Departmental Threat and Risk Assessment process through the use of an annual report on the security environment. Threats in today's environment are ever increasing. In one region visited, occupations/sit-ins/demonstrations were considered the most serious threat. The department does not have an efficient methodology to monitor its key threats, and adjust its key countermeasures if required, to ensure "acceptable" levels of risk are maintained.

The framework for the management of the security function is well established in two locations. However, a high level of security violations and breaches of sensitive and classified information persist in the department. "Low security concern" from employees is the root cause. As such, it is the department's key threat. Notwithstanding the efforts by the Security people and the many positive features of the existing management framework, security is still not sufficiently "valued" by employees.

Improvements can be cost-effectively established, departmentally and in the regions, to ensure the management framework is effective against all threats. A policy of sanctions and strengthening regional practices regarding annual security planning, allocation of sufficient resources, appropriately trained staff and a program of regular sweeps that are reported to the Regional Director General are key recommendations.

Compliance with the GSP has been strengthened since the 1992 audit and is now satisfactory in most respects. Liaison with external security agencies and e-mail security are areas which should be given attention in the future.

Background

In June 1994, Treasury Board revised the Government Security Policy (GSP). The revision took into account the current environment of security, particularly in the Information Technology (IT) area.

The Departmental Audit and Evaluation Branch (DAEB) must conduct internal audits of compliance with, and effectiveness and efficiency of the implementation of, the GSP. These audits are required at least every five years and the DAEB carried out the previous audit in 1992-1993. This audit was conducted during the period September 1996 to March 1997.

Objectives

The objectives of the audit were to review, assess and report on:

- the security management framework, that is the policies, practices and controls in place relating to security administration; and,
- compliance with, the GSP, the ITS operational standards and all departmental security policies and procedures.

Scope

The scope of the audit includes all management policies, practices, systems and controls related to the management of the security program. In addition, the scope included compliance with the GSP covering all key areas of the security program, namely:

- Information Security;
- Physical Security;
- Personnel Security;
- IT Security; and,
- Contingency Planning.

Personal safety and security of staff were included in the scope. Liaison with security agencies outside of the department (e.g. RCMP) was also included in the scope of this project but there were no visits to external agencies.

Section 2 - Observations and Recommendations

Security Environment

The departmental methodology, to monitor its key threats and adjust key countermeasures if required, needs to be strengthened to ensure "acceptable" levels of risk are maintained.

Threats in today's environment are ever-increasing. This is driven by many factors including downsizing of public and private sector organizations coupled with persistent high unemployment and technological advancement. This makes eavesdropping equipment easily accessible to the public in retail "spy" stores found in every major city.

Two years ago the department completed detailed Threat and Risk Assessments (TRAs) in all the regions and headquarters' groups. The process took over a year to complete and the results were summarized and reported to senior management in December 1994.

The departmental TRA identified threats associated with the "human element" (i.e., non-compliance with prescribed security procedures, lack of employee awareness, etc.) as the key threats to the department. We refer to this threat as "low security concern" and it was found to still be a key threat based upon our field visits and testing.

There are other threats that are now becoming more serious for the department. For example, in one region visited, **occupations/sit-ins/demonstrations** were considered a more serious threat than low security concern. Countermeasures, including reduction of reception areas and card access controls, were being adjusted to offset the increased seriousness of the threat. These countermeasures were not completed at the time of this audit such that the region was not yet within an "acceptable" level of risk.

This same region also identified employee dissatisfaction as a key threat, but a slightly less serious one than occupations/sit-ins/demonstrations. In another region, theft was considered a key threat along with its most serious threat of low security concern.

Low security concern remains the main key threat across most departmental locations. However, as other threats become as/more serious, the department is at risk by not having a more efficient method to assess and summarize key threats. The present TRA process is lengthy and complex without providing the flexibility that would allow the department to adjust their key countermeasures.

Exhibit 1, on next page, has been prepared as a sample one-page Security Environment Annual Report regions and headquarters' groups could use to efficiently assess and report on their key threats, key countermeasures, etc.

Exhibit 1

PROTECTED (when completed)

SECURITY ENVIRONMENT ANNUAL REPORT

Branch/Region: _____

Key Protection Needs	Key Threats
☐ Personnel ☐ Sensitive Information ☐ Classified Information ☐ Assets ☐ Cash, negotiables ☐ Equipment ☐ Blank Status Cards ☐ Other _____ (specify)	☐ Occupations/Sit-ins ☐ Public Access ☐ Low Security Concern ☐ Employee Dissatisfaction ☐ Bomb Threats ☐ Natural Disasters (flood, fire, etc.) ☐ Electronic Eavesdropping ☐ Other _____ (specify)

Key Countermeasures

☐ TPA Updated Annually	☐ Contingency Plans
☐ Guarding	☐ Business Resumption Plans
☐ Card Access System	☐ Security Sweeps
☐ Key Registry/Combinations	☐ IT Security Sweeps
☐ Cabinets/Containers	☐ All Violations reported to ADM/RDG/HQ
☐ Screening/Clearances Required	☐ Liaison with external Law Enforcement Agencies
☐ Training	☐ Other _____ (specify)
☐ Back-Ups Appointed	

Compliance to Prescribed Security Procedures

☐ Completely Satisfactory ☐ Satisfactory in Most Respects ☐ Unsatisfactory

Overall Risk Assessment

☐ Minimal Risk ☐ Acceptable Risk ☐ Unacceptable Risk

Action Plans

Actions Plans (where required)

_____

_____

_____

ADM/RDG name & initial _____ Date _____ DSO/RSO name & initial _____ Date _____

The Security Environment Annual Report would be prepared annually by the Regional Security Officer (RSO) or Departmental Security Officer (DSO) for headquarters' groups. It would then be reviewed and signed by a Regional Director General (RDG) or Assistant Deputy Minister (ADM).

The Security Environment Annual Report would ensure senior management is well-informed about changes in threats and allow timely action to be taken to ensure acceptable levels of risk are being maintained.

Recommendation 1: The Assistant Deputy Minister, Corporate Services should ensure the department upgrades the efficiency of the Departmental Threat and Risk Assessment process through the use of an annual report on the security environment.

Management Framework

The framework for the management of the security function is well established in two locations. However, the efforts by the Security people and the many positive features of the existing management framework have not been effective against the "low security concern" threat, which is contributing to a persistently high level of security violations and breaches of sensitive and classified information.

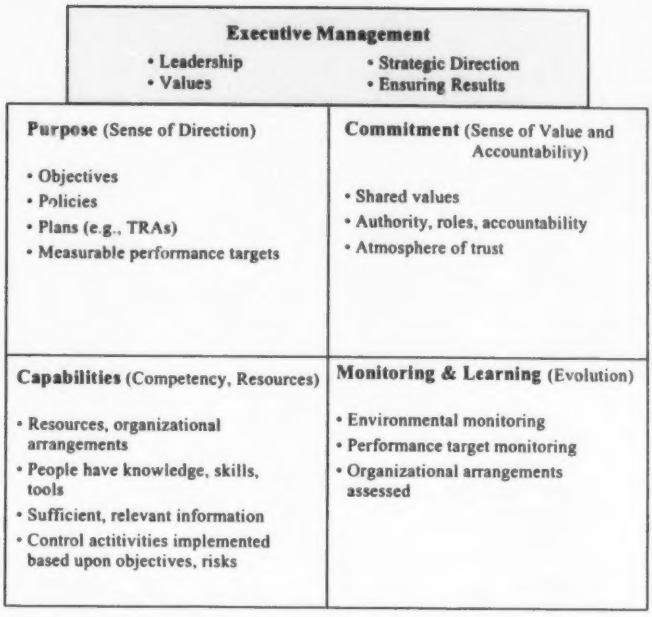
Improvements can be cost-effectively established, departmentally and in the regions, to strengthen the "value" placed on security.

We examined the department's overall management practices based upon the Management Control Framework illustrated on the following page in **Exhibit 2**.

The framework for the management of the security function departmentally includes: a comprehensive TRA process to support security planning; clear roles, responsibilities and lines of reporting for the DSO, RSOs, managers and employees, etc.; and a Departmental Security Manual which includes a Classification and Designation Guide. In addition, security staff were generally well-trained, albeit the need for training of security staff was identified in some regions visited.

The many positive features of the existing management framework have not been able to adequately address the threat of "low security concern". This threat has been identified as a key threat at headquarters and in the three regions visited. It is the direct cause of the persistently high level of security violations and breaches of sensitive and classified information. This high level of security violations was confirmed during silent hour sweeps.

Exhibit 2: Management Control Framework



At best, violations were found in 50% of work units visited — in one region it was 100% of work units swept.

In some regions, recommendations to strengthen management framework practices were made specifically to address the low security concern threat. Using the TRA methodology in annual security planning, allocating sufficient resources, establishing a program of security sweeps, reporting the results to the RDG and establishing sanctions for security violations were the major recommendations. These management framework features should be in place across the department.

Sound protection practices need to be developed as a "value" of the organization. Demonstrated senior management action is the key to illustrating the organization values security. Funding for physical access controls, support of ongoing security awareness programs and the TRAs all signal that security is valued. A policy to provide sanctions where expected practices are not taken seriously is the next concrete action senior management can take to enhance the value of security within the department. The issue of sanctions is particularly important. We also observed some documents were over-classified SECRET in the interest of ensuring their protection. Protection of a document is not assured by its marking, even a SECRET marking.

The sanctions policy, and other recommendations highlighted above can be cost-effectively implemented to strengthen the management framework. Without these changes, future violations and breaches will likely create "unacceptable" risks to the achievement of departmental objectives.

Recommendations 2: The Assistant Deputy Minister, Corporate Services should ensure:

a) a departmental policy of sanctions that may be imposed in the event of a security violation or breach is developed and communicated to all staff, and enforced;

b) the Departmental Security Officer assesses effectiveness of the sanctions policy one year after implementation; and

c) the results of the regional and headquarters' security activities and incidents are summarized annually and reported to senior management.

Recommendation 3: The Assistant Deputy Minister, Corporate Services, in consultation with Regional Director Generals should ensure the management framework for security include use of the TRA methodology in their annual security planning, allocation of sufficient resources, appropriately trained security personnel and a program of regular sweeps that are reported to the Regional Director General.

Security Program

Compliance with the GSP has been strengthened since the 1992 audit and is satisfactory in most respects. The main areas that remain of particular concern are Information Security and Contingency Planning.

Threat and Risk Assessments, Business Resumption Plans, Personnel Security, Informatics Security and Information security were all identified as requiring strengthening by the 1992 audit.

A TRA process has been developed and implemented and a project to establish Business Resumption Plans is underway at headquarters and in the regions. The Security and Emergency Measures Section at headquarters also issued guidance on contingency plans covering fire, demonstrations, bomb threats, medical emergencies and other threats in July 1997. However, in two of the three regions visited, regular liaison had not been established with external security agencies. This is an important feature of contingency planning for all regions.

The Security Services Information System (SSIS) has been implemented since the previous audit. It enables efficient processing and tracking clearances requiring updating. We also observed effective IT Security procedures in two of the three regions visited. No one had been assigned IT Security responsibility in the other region visited. (IT Security was not within the scope of our audit of headquarters security practices.)

Information Security practices observed included adequate cabinets, containers and registry arrangements in all locations visited. However, staff were consistently showing a low security concern in not ensuring sensitive and classified information was secure in silent hours. Several recommendations to address the persistent Information Security violations were made in the previous observation on management practices.

E-mail is an area of concern for Information Security. The department was pilot testing a software program to enable the e-mailing of classified and sensitive information at the time of this audit. With or without the software in place, e-mailing is becoming the transmission mode of choice and there is a need to place emphasis on e-mailing protocols in security awareness training.

The distribution of the Department's Security Manual which includes the Classification and Designation Guide is limited to a few select managers at headquarters and in the regions. The extent of this distribution may be a contributing factor to the information security deficiencies. At the time of this audit, the Security and Emergency Measures Section was considering electronic dissemination of the Security Manual to improve employee access to prescribed requirements such as those for information security.

Recommendations 4: The Departmental Security Officer should ensure:

a) security policies and procedures, including the Classification and Designation Guide, are made more accessible to employees through electronic communications; and,

b) security awareness training about the use of e-mail is given particular attention.

APPENDIX I

AREAS OF AUDIT ACTIVITY

GOVERNMENT SECURITY POLICY

Main components to assess:

- organizational structure;
- administrative procedures; and
- all sub-systems; for example:
  - Physical Security;
  - Information Technology Security;
  - Personnel/Information/Assets Security; and
  - Communications Security.

INFORMATION TECHNOLOGY SECURITY

Main components to assess:

- organizing and administering;
- personnel security;
- physical security;
- hardware security;
- software security;
- communications security; and
- operations security.

SECURITY MANAGEMENT & ADMINISTRATION FRAMEWORK

Terms of Reference

TERMS OF REFERENCE

AUDIT OF SECURITY

BACKGROUND:

In June 1994, Treasury Board revised the Government Security Policy (GSP). The revision takes account of the current environment of security, particularly in the Information Technology (IT) area.

DEPARTMENTAL SECURITY ORGANIZATION

- the Departmental Security Officer (DSO), who is appointed by the Deputy Minister, is responsible for the administration of the departmental security program consistent with the Security policy and standards;

- each Regional Security Officer (RSO) is responsible for the overall effectiveness of the security program and compliance with the GSP, the ITS standards and all the departmental policies and directives, for his/her respective region; and

- each Regional Informatics Manager (RIM) is responsible for the technical aspect pertaining to security of informatics and telecommunications within his/her region.

NEED:

The Departmental Audit and Evaluation Branch (DAEB) must conduct internal audits of compliance with, and effectiveness and efficiency of the implementation of, the GSP. These audits are required at least every five years. The Treasury Board also monitors compliance with GSP.

SCOPE:

The scope of the audit includes all management policies, practices, systems and controls related to compliance with the GSP and to the organization, management and administration of security including physical and personnel security. The areas of audit activity are listed in Appendix I.

The audit will be conducted at corporate headquarters and at British Columbia, Manitoba and the Quebec Regions.

.../2

SCOPE EXCLUSION:

The proposed audit will exclude Informatics Security at Corporate headquarters. It has been covered in the audit of Informatics and EDP Consolidation in 1995-1996 (Project 94/10).

OBJECTIVES:

The objectives of this audit are to review, assess and report on:

- compliance with, the GSP, the ITS operational standards and all departmental security policies and procedures; and
- the Security management framework, that is, the policies practices and controls in place relating to security administration.

APPROACH:

The audit will be conducted in the following three phases:

- Preliminary Survey and Evaluation;
- Fieldwork and Analysis; and
- Reporting.

RESOURCES:

The project will be implemented using contracted resources and will be managed by DAEB.

COST:

It is estimated that the contracted resources will cost between $55,000 and $66,000.

TIMEFRAME:

The audit planning will commence in August 1996 and the report will be completed by March 1997.

APPROVED BY:

B. DiBartolo
Assistant Deputy Minister
Corporate Services
August 16, 1996

Action Plan

AUDIT AND EVALUATION / VÉRIFICATION INTERNE ET ÉVALUATION

REQUEST FOR ACTION PLAN / DEMANDE DE PLAN D'ACTION

PROJECT / PROJET : 96/06
DATE SENT / DATE D'ENVOI : 97-05-12
DATE DUE / ÉCHÉANCE : 97-05-23

PROJECT TITLE / TITRE DU PROJET : Audit of Security
REGION OR BRANCH / RÉGION OU DIRECTION GÉNÉRALE : Corporate Services

(1) RECOMMENDATIONS / RECOMMANDATIONS	(2) REPORT / RAPPORT PAGE NO.	(3) ACTION PLAN / PLAN D'ACTION	(4) RESPONSIBLE MANAGER / GESTIONNAIRE RESPONSABLE (TITLE / TITRE)	(5) PLANNED COMPLETION DATE / DATE PREVUE DE MISE EN OEUVRE
1. The Assistant Deputy Minister, Corporate Services should ensure the department upgrades the efficiency of the Departmental Threat and Risk Assessment process through the use of an annual report on the security environment.	4	The proposed Annual Report will be adopted as part of the departmental security procedures and the RDGs will be requested to update the TRAs for their respective regions. A call letter will then be forwarded to all RDGs annually to request an update of the regional TRAs. The NCR TRAs will be updated in the same fashion.	Chief, SEMD	November 1, 1997
2. The Assistant Deputy Minister, Corporate Services should ensure:	6			
a) a departmental policy of sanctions that may be imposed in the event of a security violation or breach is developed and communicated to all staff, and enforced;		a) Security policy/procedures related to sanctions currently in draft; revisions still required based on recent concerns. Further consultation with Staff Relations will be initiated and security chapter will be revised/issued accordingly.	Chief, SEMD	October 31, 1997
b) the Departmental Security Officer assesses effectiveness of the sanctions policy one year after implementation; and		b) The DSO will review the impact of sanctions in one year after implementation by consulting with Staff Relations and analyzing records of violations and breaches.	Chief, SEMD	October 31, 1998
c) the results of the regional and headquarters' security activities and incidents are summarized annually and reported to senior management..		c) An annual report to the DM (c.c. Executive Committee) will be prepared based on input from all regions and will outline major security concerns and achievements during the fiscal year.	Chief, SEMD	June 30, 1997

AUDIT AND EVALUATION / VÉRIFICATION INTERNE ET ÉVALUATION

REQUEST FOR ACTION PLAN / DEMANDE DE PLAN D'ACTION

PROJECT / PROJET : 96/06
DATE SENT / DATE D'ENVOI : 97-05-12
DATE DUE / ÉCHÉANCE : 97-05-23

PROJECT TITLE / TITRE DU PROJET : Audit of Security
REGION OR BRANCH / RÉGION OU DIRECTION GÉNÉRALE : Corporate Services

(1) RECOMMENDATIONS / RECOMMANDATIONS	(2) REPORT / RAPPORT PAGE NO.	(3) ACTION PLAN / PLAN D'ACTION	(4) RESPONSIBLE MANAGER / GESTIONNAIRE RESPONSABLE (TITLE / TITRE)	(5) PLANNED COMPLETION DATE / DATE PREVUE DE MISE EN OEUVRE
3. The Assistant Deputy Minister, Corporate Services, in consultation with Regional Director Generals should ensure the management framework for security include use of the TRA methodology in their annual security planning, allocation of sufficient resources, appropriately trained security personnel and a program of regular sweeps that are reported to the Regional Director General.	6	The DSO will consult with the RDGs, Directors of Corporate Services and RSOs in an attempt to develop a departmental approach that could improve the management framework and participation/involvement in the regions. The DSO will also solicit their full support/participation in developing and implementing a departmental plan.	Chief, SEMD	January 31, 1998

AUDIT AND EVALUATION / VÉRIFICATION INTERNE ET ÉVALUATION

REQUEST FOR ACTION PLAN / DEMANDE DE PLAN D'ACTION

PROJECT / PROJET : 96/06
DATE SENT / DATE D'ENVOI : 97-05-12
DATE DUE / ÉCHÉANCE : 97-05-23

PROJECT TITLE / TITRE DU PROJET : Audit of Security
REGION OR BRANCH / RÉGION OU DIRECTION GÉNÉRALE : Administrative Services

(1) RECOMMENDATIONS / RECOMMANDATIONS	(2) REPORT / RAPPORT PAGE NO.	(3) ACTION PLAN / PLAN D'ACTION	(4) RESPONSIBLE MANAGER / GESTIONNAIRE RESPONSABLE (TITLE / TITRE)	(5) PLANNED COMPLETION DATE / DATE PREVUE DE MISE EN OEUVRE
4. The Departmental Security Officer should ensure:	7			
c) security policies and procedures, including the Classification and Designation Guide, are made more accessible to employees through electronic communications; and,		a) Intranet site to be used for this purpose, when available. SEMD will contact the Intranet Coordinator to determine departmental plan/time frame and requirements. If time frame acceptable, SEMD will pursue this initiative separately in consultation with the Departmental Intranet Coordinator.	Chief, SEMD	December 31, 1997
d) security awareness training about the use of e-mail is given particular attention.		b) Transmission of designated/classified information by e-mail has been addressed through the Network Security Strategy recently approved by IMC.	Chief, SEMD and IMB	2 year implementation (June 30, 1999)
		The regular use of e-mail and associated security concerns are currently being presented during the security briefings. Briefing material will formally be revised to address this issue.	Chief, SEMD	September 30,1997
		An article will also be included in the next Security Bulletin	Chief, SEMD	July 31, 1997

Ministère des Affaires indiennes et du Nord canadien
Direction générale de l'évaluation et de la vérification interne

Rédigé par :

Hasan Zaidi, Gestionnaire de la vérification
Hélène Thériault, Agent des projets de vérification
Direction générale de l'évaluation et de la vérification interne

Assisté par :
Performance Management Network

Vérification de la sécurité

Projet 96/06
Juin 1997

Table des matières

Page

Sommaire ..... **i**
- Objet i
- Contexte i
- Évaluation globale i
- Principales observations i

Section 1 - Introduction **1**
- Contexte 1
- Objectifs 1
- Portée 1

Section 2 - Observations et recommandations **2**
- Environnement de la sécurité 2
- Cadre de gestion 5
- Programme de sécurité 7

Annexe 1 10

Annexes
- Mandat
- Plan d'action

Sommaire

Objet

La présente vérification a pour objet d'examiner systématiquement la gestion et l'administration de la fonction sécurité au Ministère ainsi que la conformité avec la Politique et les normes sur la sécurité (PNS) et les normes opérationnelles de la sécurité des technologies de l'information (STI).

Contexte

Tous les cinq ans, le Ministère doit procéder à des vérifications internes pour déterminer dans quelle mesure la PNS est respectée et pour établir si celle-ci est appliquée de manière efficace et efficiente. La vérification effectuée en 1992-1993 avait conclu à la nécessité d'améliorer les méthodes de gestion et d'exécution de la fonction afin de respecter les exigences de la PNS.

Évaluation globale

La fonction sécurité au Ministère s'est améliorée par rapport à ce qui avait été observé lors de la vérification de 1992. Ceci est principalement dû à l'établissement d'évaluations de la menace et des risques, de programmes de sensibilisation à la sécurité et autres initiatives connexes. Cependant, dans la plupart des endroits visités, les vérificateurs ont établi que la préoccupation pour la sécurité demeure faible et que, par conséquent, les biens, en particulier les renseignements de nature délicate, n'étaient pas protégés de façon acceptable.

Pour amener la sécurité à un niveau acceptable il faudra bien sûr modifier les procédures, mais surtout amener les gens à modifier leurs attitudes.

Principales observations

Le Ministère se doit d'améliorer l'efficacité de son processus annuel d'évaluation de la menace et des risques avec l'utilisation d'un rapport annuel sur la sécurité. Aujourd'hui, la menace est en progression constante. Dans l'une des régions visitées, la principale menace réside dans les occupations et les manifestations. Le Ministère ne dispose pas d'une méthode efficace pour évaluer les situations qui représentent pour lui une menace et pour rectifier au besoin ses contre-mesures de manière à assurer un niveau de risque «acceptable».

Le cadre de gestion de la sécurité est bien établi dans deux services. Cependant, le nombre d'infractions et de manquements à la sécurité des renseignements classifiés et de nature délicate est encore très élevé au Ministère. «La faible préoccupation des employés pour la sécurité» est la principale cause de cette situation et de ce fait la principale menace pour le Ministère. Malgré tous les efforts des responsables de la sécurité et les nombreux éléments positifs du cadre de gestion actuel, la sécurité n'est pas toujours suffisamment "valorisée" par les employés.

Il serait possible d'apporter, à peu de frais, à l'Administration centrale et dans les régions, des améliorations qui rendraient le cadre de gestion efficace contre tous les types de menaces. Les recommandations clefs portent sur l'établissement d'une politique de sanctions, le renforcement des pratiques régionales en matière de planification annuelle de la sécurité, l'attribution de ressources suffisantes, la formation du personnel et la mise sur pied d'un programme de ratissages périodiques dont les résultats seraient communiqués au directeur général régional.

Depuis la vérification de 1992, la conformité au PNS s'est accrue et est actuellement satisfaisante, de façon générale. La liaison avec les organismes de sécurité de l'extérieur et la sécurité du courrier électronique sont des domaines qui devraient retenir l'attention dans l'avenir.

Contexte

En juin 1994, le Conseil du Trésor a révisé la Politique et les normes sur la sécurité (PNS) en tenant compte de l'environnement actuel de la sécurité, et en particulier celle de la technologie de l'information (TI).

Tous les cinq ans, la Direction générale de l'évaluation et de la vérification interne (DGÉVI) doit effectuer des vérifications internes pour déterminer si le Ministère se conforme à la PNS et si celle-ci est appliquée de manière efficace et efficiente. L'avant dernière évaluation remonte à 1992-1993 et celle qui est visée par le présent rapport a été effectuée entre les mois de septembre 1996 et de mars 1997.

Objectifs

La vérification avait pour objectifs d'examiner et d'évaluer les questions suivantes.

- le cadre de gestion de la sécurité, à savoir les politiques, les pratiques et les contrôles existants en matière d'administration de la sécurité;

- le respect de la PNS, des normes d'exploitation des STI et de l'ensemble des politiques et des procédures ministérielles en matière de sécurité.

Portée

La vérification a porté sur toutes les pratiques et politiques de gestion et sur tous les systèmes et contrôles relatifs à la gestion du programme de sécurité, de même que sur le respect de la PNS par l'intermédiaire d'un examen des principaux volets du programme, à savoir :

- la sécurité de l'information;
- la sécurité du matériel;
- la sécurité du personnel;
- la sécurité de la TI;
- les plans d'urgence.

La sécurité personnelle des employés était aussi un élément de cette vérification de même que l'examen de la liaison avec les organismes de l'extérieur (p. ex. GRC), mais aucune visite n'a été effectuée auprès de tels organismes.

Section 2 - Observations et recommandations

Environnement de la sécurité

La méthode du Ministère pour évaluer les menaces auxquelles il est exposé et pour rectifier ses contre-mesures au besoin se doit d'être améliorée pour assurer un niveau de risque «acceptable».

Beaucoup de facteurs dont la réduction des effectifs dans les secteurs public et privé, les progrès technologiques et la persistance du chômage à un niveau élevé font que la menace est en progression constante. Par ailleurs, quiconque le désire peut facilement se procurer du matériel d'écoute dans la plupart des magasins de détail spécialisés de toutes les grandes villes.

Il y a deux ans, le Ministère a effectué une évaluation détaillée de la menace et des risques (EMR) dans tous ses bureaux régionaux et à l'Administration centrale. Le résumé des résultats de cette évaluation, qui s'est échelonnée sur une période d'un an, a été communiqué à la haute direction en décembre 1994.

L'EMR effectuée par le Ministère montre que les facteurs liés à l'«élément humain» (p. ex. non-respect des procédures de sécurité et manque de sensibilisation des employés) constituent la principale menace pour l'organisation. Nous appelons cette menace «faible préoccupation pour la sécurité» et nous avons constaté lors de nos visites et de nos évaluations sur le terrain qu'elle constitue encore une des principales menaces pour le Ministère.

D'autres menaces deviennent de plus en plus graves pour le Ministère. Par exemple, dans l'une des régions visitée les **occupations et les manifestations** étaient considérées comme posant une menace plus grande que la faible préoccupation pour la sécurité. Pour compenser l'accroissement de la gravité de la menace, les autorités ont entrepris de rectifier les contre-mesures, par exemple en diminuant le nombre d'aires d'accueil et en installant des systèmes de contrôle des accès par carte. Au moment où nous avons effectué la présente vérification, ces mesures n'étaient pas encore achevées, de sorte que le niveau de risque dans cette région était encore «inacceptable».

Toujours dans cette région, on avait établi que le degré d'insatisfaction des employés constituait une menace, quoique légèrement moins grande que les occupations et manifestations. Dans une autre région, le vol était considéré comme une des principales menaces, au même titre que la faible préoccupation pour la sécurité, qui vient au premier rang.

La faible préoccupation pour la sécurité demeure la principale menace dans la plupart des services du Ministère. Cependant, au vu du fait que les autres menaces deviennent aussi grandes ou plus grandes, le Ministère s'expose à des risques puisqu'il ne possède pas de méthode pour évaluer les principales menaces et faire le point à ce sujet. Le processus actuel d'évaluation de la menace et des risques est complexe et fastidieux, et il n'offre pas la souplesse qui permettrait au Ministère d'adapter ses contre-mesures.

La **pièce 1** présente un modèle de Rapport annuel sur la sécurité que les régions et l'Administration centrale pourraient utiliser pour évaluer efficacement les menaces auxquelles elles sont exposées, pour préciser les contre-mesures prises, pour faire rapport, etc.

Le rapport annuel sur la sécurité serait rempli par l'agent régional de la sécurité (ARS), pour les bureaux régionaux, ou par l'agent ministériel de la sécurité (AMS), pour l'Administration centrale, et serait ensuite présenté au directeur général régional (DGR) ou au sous-ministre adjoint (SMA) pour examen et signature.

Grâce au rapport annuel sur la sécurité, la haute direction serait constamment au courant des changements survenus en ce qui a trait aux divers types de menaces et pourrait réagir rapidement pour assurer le maintien d'un niveau de risque acceptable.

Recommandation 1 : Le sous-ministre adjoint, Services ministériels, devrait veiller à ce que le Ministère implante un Rapport annuel sur la sécurité de façon à améliorer le processus d'évaluation de la menace et des risques.

Pièce 1

PROTÉGÉ (lorsque rempli)

RAPPORT ANNUEL SUR LA SÉCURITÉ

Direction générale / région : _____

Besoins en matière de protection	Menaces
☐ Personnel ☐ Renseignements de nature délicate ☐ Renseignements classifiés ☐ Biens ☐ Espèces, effets négociables ☐ Matériel ☐ Certificats de statut d'Indien ☐ Autres _____ (préciser)	☐ Occupations/manifestations sur le tas ☐ Accès du public ☐ Faible préoccupation pour la sécurité ☐ Insatisfaction des employés ☐ Bombes ☐ Catastrophes naturelles (inondations, incendies, etc.) ☐ Écoute électronique ☐ Autres _____ (préciser)

Contre-mesures	
☐ Mise à jour annuelle des EMR	☐ Plans d'urgence
☐ Gardiennage	☐ Plans de reprise des activités
☐ Système de contrôle d'accès par cartes	☐ Ratissages de sécurité
☐ Registre des clés/cadenas ou serrures à combinaison	☐ Ratissages de sécurité (TI)
☐ Classeurs/conteneurs	☐ Signaler toute infraction au SMA, au DGR ou à l'AC
☐ Autorisations de sécurité exigées	☐ Liaison avec les organismes extérieurs d'application de la loi
☐ Formation	☐ Autres _____ (préciser)
☐ Nomination de suppléants	

Respect des procédures de sécurité		
☐ Entièrement satisfaisant	☐ Satisfaisant	☐ Insatisfaisant

Évaluation globale du risque		
☐ Minimal	☐ Acceptable	☐ Inacceptable

Plans d'action

Plans d'action (s'il y a lieu) :

_____

_____

_____

_____ _____ _____ _____

SMA/DGR nom et initiales — Date — AMS/ARS nom et initiales — Date

Cadre de gestion

Le cadre de gestion de la sécurité est bien établi dans deux services. Cependant les efforts des responsables de la sécurité et les nombreux éléments positifs du cadre actuel de gestion n'ont pas réussi à contrer la menace que présente la «faible préoccupation pour la sécurité», laquelle contribue a maintenir à un niveau élevé le nombre d'infractions et de manquements à la sécurité des renseignements classifiés et de nature délicate.

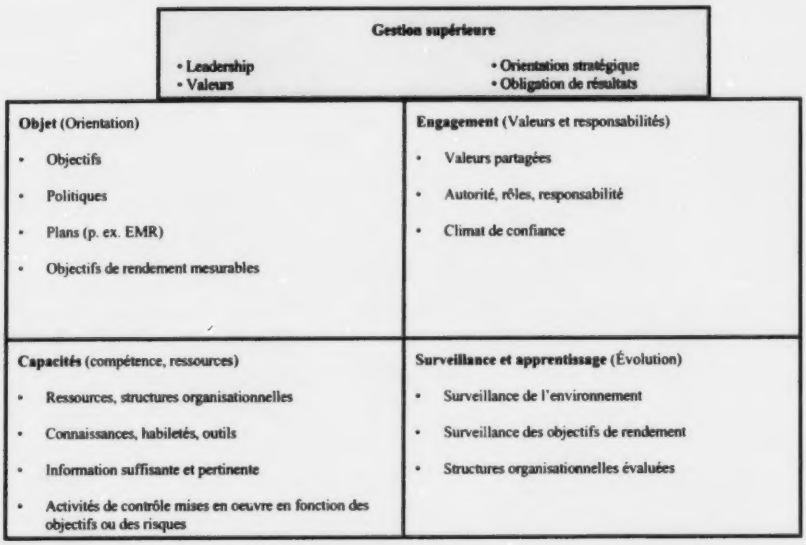
Il serait possible de modifier à peu de frais les pratiques existantes à l'Administration centrale et dans les régions pour «valoriser» davantage la fonction sécurité.

Nous avons examiné l'ensemble des pratiques de gestion du Ministère en matière de sécurité à la lumière du cadre de gestion présenté à la page suivante **(pièce 2)**.

Le cadre de gestion de la sécurité au Ministère comprend : un processus exhaustif d'EMR à l'appui de la planification de la sécurité; des rôles, des responsabilités et des canaux hiérarchiques bien définis pour l'AMS, l'ARS, les gestionnaires et les employés, etc.; ainsi qu'un Manuel de la sécurité qui comprend un Guide de classification et de désignation. En outre, si le personnel préposé à la sécurité est en général bien formé, nous avons relevé quelques lacunes à cet égard dans certaines des régions que nous avons visitées.

Les nombreux éléments positifs du cadre de gestion actuel n'ont pu remédier convenablement à la menace que présente la faible préoccupation pour la sécurité, laquelle a été observée tant à l'Administration centrale que dans les régions visitées. Cette menace est la cause directe du nombre encore élevé d'infractions et de manquements à la sécurité des renseignements classifiés et de nature délicate. Ces manquements ou infractions à la sécurité ont d'ailleurs été confirmés au cours des ratissages effectués en dehors des heures de travail.

Pièce 2 : Cadre de gestion



Dans le meilleur des cas, des manquements ont été constatés dans 50 % des services visités. Dans une région, on a relevé des infractions dans tous les services.

Dans certaines régions, on a recommandé que des mesures de renforcement du cadre de gestion soient prises précisément pour régler le problème que représente la faible préoccupation à l'égard de la sécurité. On a aussi recommandé de recourir au processus d'évaluation de la menace et des risques dans le cadre de la planification annuelle de la sécurité, d'affecter à cette fonction des ressources suffisantes, de mettre sur pied un programme de ratissages de sécurité, de communiquer les résultats de ce dernier au DGR, et enfin d'impose des sanctions dans les cas de manquement ou d'infraction. Ces éléments du cadre de gestion devraient être mis en place dans tous les services du Ministère.

Il faut établir de saines pratiques en matière de sécurité et faire de celle-ci une «valeur» de l'organisation. L'engagement des membres de la haute direction à l'égard de la sécurité est essentiel pour montrer l'importance que l'organisation accorde à cette fonction. L'octroi d'un financement pour les mesures de contrôle d'accès physique, l'établissement d'un programme permanent de sensibilisation à la sécurité et la réalisation des EMR sont autant de mesures qui montrent qu'on se préoccupe de la sécurité. L'adoption d'une politique prévoyant l'imposition de sanctions dans les cas où les pratiques préconisées ne sont pas prises au sérieux est la deuxième mesure concrète que la haute direction peut prendre pour valoriser davantage la fonction sécurité au Ministère. La question des sanctions est particulièrement importante. Nous avons noté que certains documents étaient abusivement classifiés SECRET pour en assurer la protection. La protection d'un document n'est pas assurée du simple fait de lui attribuer une cote de sécurité, fut-elle de niveau SECRET.

La politique de sanctions et les autres recommandations énumérées ci-dessus peuvent être mises en oeuvre à peu de frais pour renforcer le cadre de gestion. À défaut d'agir maintenant, les manquements et les infractions qui pourront se produire dans l'avenir auront vraisemblablement pour effet de créer des risques «inacceptables» eu égard à l'atteinte des objectifs du Ministère.

Recommandation 2 : Le sous-ministre adjoint, Services ministériels, devrait s'assurer :

a) que l'on élabore une politique ministérielle d'imposition de sanctions en cas de manquement ou d'infraction à la sécurité, qu'on la communique à tout le personnel et qu'on la mette en application;

b) que l'agent ministériel de la sécurité (AMS) évalue l'efficacité de la politique de sanctions un an après sa mise en oeuvre;

c) que l'on fasse le point annuellement, dans un rapport à la haute direction, sur les incidents liés à la sécurité et les résultats des activités de sécurité dans les bureaux régionaux et à l'Administration centrale.

Recommandation 3 : Le sous-ministre adjoint, Services ministériels, de concert avec les directeurs généraux régionaux, devrait s'assurer que le cadre de gestion de la sécurité prévoit la réalisation d'évaluations de la menace et des risques dans le cadre de la planification annuelle de la sécurité, l'affectation de ressources suffisantes, une formation adéquate du personnel et l'établissement d'un programme de ratissages périodiques dont les résultats devront être communiqués au directeur général régional.

Programme de sécurité

Depuis la vérification effectuée en 1992, la PNS est, en règle générale, respectée de façon satisfaisante. Cependant, deux domaines, à savoir la sécurité de l'information et la planification d'urgence, restent sources d'inquiétudes.

D'après le rapport de vérification de 1992, les activités liées aux évaluations de la menace et des risques, aux plans de reprise des activités, à la sécurité du personnel, à la sécurité informatique et à la sécurité de l'information doivent être renforcées.

Un processus d'évaluation de la menace et des risques a été élaboré et mis en oeuvre et un projet visant à établir des plans de reprise des activités est en cours à l'Administration centrale et dans les régions. En outre, la Section de la sécurité et des mesures d'urgence, à l'Administration centrale, a publié en juillet 1997 un document qui traite des plans d'intervention en cas d'incendie, de manifestations, d'appels à la bombe, d'urgences médicales et d'autres menaces. Cependant, dans deux des trois régions visitées, des contacts réguliers n'avaient pas été établis avec des organismes de sécurité de l'extérieur. Or, il s'agit d'un élément important des plans d'intervention pour toutes les régions.

Depuis la dernière vérification, on a mis en oeuvre un système d'information sur les services de sécurité (SISS) qui permet de suivre et de traiter efficacement les autorisations de sécurité qui nécessitent une mise à jour. Nous avons également observé que des procédures efficaces pour assurer la sécurité de la TI étaient en place dans deux des trois régions visitées. Dans l'autre région où nous nous sommes rendus, personne n'avait été désigné comme responsable de la sécurité de la TI. (La sécurité de la TI ne faisait pas partie de notre mandat de vérification des pratiques de sécurité à l'Administration centrale).

Dans tous les endroits que nous avons visités, des mesures avaient été prises (p. ex. installations de classeurs et de conteneurs adéquats et instauration de procédures d'enregistrement) pour accroître la sécurité de l'information. Cependant, nous avons constaté que presque tout le personnel faisait preuve d'une faible préoccupation à l'égard de la sécurité en ne protégeant pas les renseignements classifiés et de nature délicate en dehors des heures de travail. Plusieurs recommandations visant à régler le problème persistant des manquements à la sécurité de l'information ont été faites dans les observations antérieures relatives aux pratiques de gestion.

Le courrier électronique est à l'origine de préoccupations en matière de sécurité de l'information. Lors de notre vérification, le Ministère était à mettre à l'essai un logiciel capable de transmettre par courrier électronique des renseignements classifiés et de nature délicate. Peu importe que ce logiciel soit adopté ou non, le courrier électronique s'impose de plus en plus comme le mode de transmission privilégié. C'est pourquoi il est nécessaire, dans les cours de sensibilisation à la sécurité, de mettre l'accent sur les protocoles de communication par courrier électronique.

La distribution du manuel de la sécurité, qui comprend un guide de classification et de désignation, est limitée à un nombre restreint de gestionnaires choisis à l'Administration centrale et dans les régions. C'est peut-être ce qui explique les lacunes en matière de sécurité de l'information. Au moment de la vérification, la section de la sécurité et des mesures d'urgence examinait la possibilité de diffuser électroniquement le manuel pour permettre aux employés d'avoir accès aux exigences prescrites, notamment au titre de la sécurité de l'information.

Recommandation 4 : L'agent ministériel de la sécurité (AMS) devrait s'assurer :

a) que les politiques et les procédures en matière de sécurité, y compris le Guide de classification et de désignation, soient rendues plus accessibles aux employés par l'intermédiaire des communications électroniques;

b) que l'on attache une importance particulière à la formation sur l'utilisation du courrier électronique dans le cadre de la sensibilisation à la sécurité.

ANNEXE 1

CHAMPS DE L'ACTIVITÉ VÉRIFICATION

POLITIQUE GOUVERNEMENTALE SUR LA SÉCURITÉ

Principales composantes à évaluer :

- structure organisationnelle;
- procédures administratives;
- tous les sous-systèmes; par exemple :
  - sécurité des lieux
  - sécurité des technologies de l'information
  - sécurité du personnel/de l'information/des biens
  - sécurité des communications

SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

Principales composantes à évaluer :

- organisation et administration;
- sécurité du personnel;
- sécurité des lieux;
- sécurité du matériel;
- sécurité des logiciels;
- sécurité des communications;
- sécurité des opérations.

CADRE DE GESTION ET CADRE D'ADMINISTRATION DE LA SÉCURITÉ

Mandat

MANDAT

VÉRIFICATION DE LA SÉCURITÉ

CONTEXTE : En juin 1994, le Conseil du Trésor a révisé la Politique et les normes sur la sécurité (PNS) d'une façon qui tient compte de l'environnement actuel de la sécurité, et plus particulièrement des technologies de l'information.

ORGANISATION DES ACTIVITÉS LIÉES À LA SÉCURITÉ AU MINISTÈRE

- le responsable de la sécurité au Ministère (RSM), nommé par le sous-ministre, veille à ce que le programme ministériel en matière de sécurité soit administré conformément à la PNS;
- l'agent régional de la sécurité (ARS) veille à l'efficacité générale du programme sur la sécurité ainsi qu'au respect de la PNS, des normes de sécurité de la technologie de l'information et de toutes les politiques et directives ministérielles dans sa région;
- le gestionnaire régional de la sécurité (GRS) est responsable des aspects techniques de la sécurité informatique et de la sécurité des télécommunications dans sa région.

JUSTIFICATION : La DGÉVI doit effectuer des vérifications internes pour déterminer si le Ministère se conforme à la PNS et si celle-ci est appliquée de manière efficace et efficiente. Ces vérifications doivent être faites au moins tous les cinq ans. De plus, le Conseil du Trésor veille à ce que la PNS soit respectée.

PORTÉE : La vérification englobe toutes les politiques de gestion, les pratiques, les systèmes et les contrôles relatifs au respect de la PNS, ainsi que l'organisation, la gestion et l'administration de la sécurité, y compris la sécurité des lieux et la sécurité du personnel. Les secteurs visés par l'activité de vérification sont énumérés à l'annexe 1.

La vérification sera effectuée à l'Administration centrale du Ministère et dans les régions de la Colombie-Britannique, du Manitoba et du Québec.

EXCLUSION : La vérification proposée ne portera pas sur la sécurité informatique à l'Administration centrale, couverte par la Vérification de l'informatique et du regroupement des installations du traitement électronique des données, en 1995-1996 (projet 94/10).

.../2

OBJECTIFS : La vérification vise à examiner et à évaluer les éléments suivants et à faire rapport à leur sujet :

- la conformité avec la PNS, les normes opérationnelles de STI et l'ensemble des politiques et procédures ministérielles concernant la sécurité;
- le cadre de gestion de la sécurité, soit les politiques et les contrôles en place reliés à l'administration de la sécurité.

DÉMARCHE : La vérification suivra les trois étapes suivantes :

- examen et évaluation préliminaires;
- travail sur le terrain et analyse;
- rapport.

RESSOURCES : Le projet sera dirigé par la DGÉVI et réalisé avec l'aide de ressources contractuelles.

COÛT : On estime que le projet coûtera entre 55 000 $ et 66 000 $.

CALENDRIER : Les travaux de planification débuteront en août 1996, et le rapport sera terminé en mars 1997.

APPROUVÉ PAR :

B. DiBartolo
Sous-ministre adjoint
Services ministériels
le 16 août 1996

Plan d'action

AUDIT AND EVALUATION / VERIFICATION INTERNE ET ÉVALUATION

REQUEST FOR ACTION PLAN / DEMANDE DE PLAN D'ACTION

PROJECT / PROJET : 96/06
DATE SENT / DATE D'ENVOI : 97.05.12
DATE DUE / ÉCHÉANCE : 97.05.23

PROJECT TITLE / TITRE DU PROJET : Vérification de la sécurité
REGION OR BRANCH / RÉGION OU DIRECTION GÉNÉRALE : Services ministériels

(1) RECOMMENDATIONS / RECOMMANDATIONS	(2) REPORT / RAPPORT PAGE NO.	(3) ACTION PLAN / PLAN D'ACTION	(4) RESPONSIBLE MANAGER / GESTIONNAIRE RESPONSABLE (TITLE / TITRE)	(5) PLANNED COMPLETION DATE / DATE PREVUE DE MISE EN OEUVRE
1. Le sous-ministre adjoint, Services ministériels, devrait veiller à ce que le Ministère implante un Rapport annuel sur la sécurité de façon à améliorer le processus d'évaluation de la menace et des risques.	3	Le rapport annuel proposé sera adopté et intégré aux procédures ministérielles sur la sécurité et les DGR devront mettre à jour les EMR de leurs régions respectives. Chaque année, une lettre d'appel sera envoyée aux DGR afin de leur demander de mettre à jour leur EMR. L'EMR pour la RCN sera mise à jour de la même façon.	Chef, DSMU	01-11-97
2. Le sous-ministre adjoint, Services ministériels, devrait s'assurer : a) que l'on élabore une politique ministérielle d'imposition de sanctions en cas de manquement ou d'infraction à la sécurité, qu'on la communique à tout le personnel et qu'on la mette en application; b) que l'agent ministériel de la sécurité (AMS) évalue l'efficacité de la politique de sanctions un an après sa mise en oeuvre; c) que les incidents liés à la sécurité et que les résultats des activités de sécurité dans les bureaux régionaux et à l'Administration centrale soient présentés à la haute direction dans un rapport récapitulatif.	7	a) La politique sur la sécurité et les procédures de sécurité sont actuellement en voie de rédaction afin d'y intégrer des dispositions sur les sanctions; celles-ci devront être modifiées pour tenir compte des préoccupations soulevées. On entreprendra d'autres consultations avec les Relations de travail et le chapitre sur la sécurité sera révisé et diffusé par la suite. b) L'AMS étudiera les répercussions des sanctions un an après leur mise en application en consultant les Relations de travail et en analysant les cas de manquements et d'infractions à la sécurité. c) Un rapport annuel au SM (avec copie conforme au comité de la haute direction) sera rédigé d'après les informations fournies par les régions. Il fera état des incidents majeurs liés à la sécurité ainsi que des réalisations au cours de l'année financière.	Chef, DSMU Chef, DSMU Chef, DSMU	31-10-97 31-10-98 30-06-97

AUDIT AND EVALUATION / VERIFICATION INTERNE ET ÉVALUATION

REQUEST FOR ACTION PLAN / DEMANDE DE PLAN D'ACTION

PROJECT / PROJET : 96/06
DATE SENT / DATE D'ENVOI : 97.05.12
DATE DUE / ÉCHÉANCE : 97.05.23

PROJECT TITLE / TITRE DU PROJET : Vérification de la sécurité
REGION OR BRANCH / RÉGION OU DIRECTION GÉNÉRALE : Services ministériels

(1) RECOMMENDATIONS / RECOMMANDATIONS	(2) REPORT / RAPPORT PAGE NO.	(3) ACTION PLAN / PLAN D'ACTION	(4) RESPONSIBLE MANAGER / GESTIONNAIRE RESPONSABLE (TITLE / TITRE)	(5) PLANNED COMPLETION DATE / DATE PRÉVUE DE MISE EN OEUVRE
3. Le sous-ministre adjoint, Services ministériels, de concert avec les directeurs généraux régionaux, devrait s'assurer que le cadre de gestion de la sécurité prévoit l'exécution d'évaluations de la menace et des risques dans le contexte de la planification annuelle de la sécurité, l'attribution de ressources suffisantes, la mise sur pied d'activités adéquates de formation du personnel et l'établissement d'un programme de ratissages périodiques dont les résultats devront être communiqués au directeur général régional.	7	L'AMS consultera les DGR, les directeurs des Services ministériels et les ARS dans le but d'établir une ligne de conduite ministérielle pouvant améliorer le cadre de gestion et la participation des régions. Il leur demandera également de participer activement à l'établissement et à la mise en application d'un plan ministériel.	Chef, DSMU	31-01-98

AUDIT AND EVALUATION / VERIFICATION INTERNE ET ÉVALUATION

REQUEST FOR ACTION PLAN / DEMANDE DE PLAN D'ACTION

PROJECT / PROJET : 96/06
DATE SENT / DATE D'ENVOI : 97.05.12
DATE DUE / ÉCHÉANCE : 97.05.23

PROJECT TITLE / TITRE DU PROJET : Vérification de la sécurité
REGION OR BRANCH / RÉGION OU DIRECTION GÉNÉRALE : Services administratifs

(1) RECOMMENDATIONS / RECOMMANDATIONS	(2) REPORT / RAPPORT PAGE NO.	(3) ACTION PLAN / PLAN D'ACTION	(4) RESPONSIBLE MANAGER / GESTIONNAIRE RESPONSABLE (TITLE / TITRE)	(5) PLANNED COMPLETION DATE / DATE PREVUE DE MISE EN OEUVRE
4. L'agent ministériel de la sécurité (AMS) devrait s'assurer :	9			
a) que les politiques et les procédures en matière de sécurité, y compris le Guide de classification et de désignation, soient rendues plus accessibles aux employés par l'intermédiaire des communications électroniques;		a) Le site Intranet sera utilisé à cette fin, lorsqu'il sera fonctionnel. La SSMU communiquera avec le coordonnateur de l'Intranet afin de connaître le plan ministériel, le calendrier d'application et les exigences liés à ce site. Si le calendrier d'application convient, la SSMU poursuivra cette initiative séparément en consultation avec le coordonnateur du site Intranet pour le Ministère.	Chef, DSMU	31-12-97
b) que l'on attache une importance particulière à la formation sur l'utilisation du courrier électronique dans le cadre de la sensibilisation à la sécurité.		b) La question de la transmission d'information classifiée par courrier électronique a été abordée dans la Stratégie sur la sécurité du réseau que le CGI vient d'approuver.	Chef, DSMU et DGGI	Mise en oeuvre échelonnée sur deux ans (30-06-99)
		L'utilisation courante du courrier électronique et les préoccupations touchant la sécurité qui en découlent font partie des présentations données dans le cadre des séances d'information sur la sécurité. Le contenu de ces séances sera révisé pour tenir compte de cette question.	Chef, DSMU	30-09-97
		Un article à ce sujet paraîtra également dans le prochain numéro du Bulletin sur la sécurité.	Chef, DSMU	31-07-97